

Websense 2008 Security Threat Predictions

Websense 2008 Security Threat Predictions

Introduction

This Security Threat Predictions report summarizes the predictions of Websense Security Labs, the security research arm of Websense that discovers and investigates today's advanced Internet threats and publishes its findings globally. Organizations around the world rely on Websense to best protect employees, critical applications and confidential data from increasingly sophisticated and dangerous Internet threats. The predictions contained within this report are based on analysis of current attack trends, cyber criminal techniques and threat intelligence gathered by researchers with Websense ThreatSeeker™ technology. ThreatSeeker scans more than 600 million Web sites per week searching for malicious code, along with Websense's On Demand Services, which scans more than 350 million emails per week for email security threats.

Summary

Websense Security Labs™ finds that cyber criminal techniques are evolving quickly and efficiently to not only evade detection, but to steal data and manipulate trusted content such as Web site and applications. As such, it is becoming even more critical for organizations and individuals to recognize that attackers are changing techniques and launching targeted attacks.

Websense Security Labs expects to see the following in 2008:

- The Olympics will spur a flurry of hacker activity such as compromises of popular Olympic news or other sports sites
- Special interest groups that fall within a certain age group, wealth bracket, or people with particular purchasing habits, will become a target of Web 2.0 attacks
- Spam will increase in the blogosphere and "talk back" sections of news sites to drive traffic and increase search engine rankings of infected Web sites.

Top 10 Security Threat Predictions

1. Olympics – new cyber attacks, phishing and fraud

Event-based attacks and scams are popular, and with the whole world watching, the 2008 Olympics may fuel a surge in cyberattacks. As the Olympic torch burns, Websense researchers predict the possibility of large scale denial of service attacks on Beijing Olympic-related sites as political statements and fraud attempts through email and the Web surrounding the Olympics. Additionally, Websense predicts compromises of popular Olympic news or other sports sites — attacks designed to install malicious code on end-users machines and steal personal or business confidential information.

2. Cross platform Web attacks – Mac, iPhone popularity spurs increase

With the brand popularity and growing use of iPhones and Macintosh computers, Websense researchers predict attackers will increasingly launch cross-platform Web attacks that detect the operating system in use and serve up code specifically targeting that operating system instead of attacks based on just the Web browser. Operating systems that are targeted now include Mac OSX, iPhone, and Windows.

3. Malicious SPAM invades blogs, search engines, forums and Web sites

Websense predicts that hackers will increasingly use Web spam to post URLs to malicious sites within forums, blogs, in the commentary or “talk-back” sections of news sites and on compromised Web sites. This activity not only drives traffic to the infected Web sites but also assists in the purveyor’s site sitting higher on search engine rankings, increasing the risk that users will visit the site.

4. Attackers use Web’s ‘weakest links’ to launch attacks

The Web is an entanglement of links and content. The advent of Web 2.0 additions such as Google AdSense, mash-ups, widgets, and social networks along with the massive amounts of Web advertisements linked to Web pages have increased the likelihood of ‘weak links’—or Web sites and content that are vulnerable to compromises. Websense predicts that attackers will increasingly exploit the weakest links within the Web infrastructure in order to target the greatest number of Internet users. Most vulnerable to these attacks are search engines and large user networks such as MySpace, Facebook or other social networking sites.

5. Number of compromised Web sites will surpass number of created malicious sites

The Web as an attack vector has been steadily increasing for the last five years and now attackers are using compromised sites as their launching platforms—even more than their own created sites. Compromising sites—particularly, sites well-visited by end-users, such as the Dolphin Stadium attack that occurred a few days prior to the 2007 [Super Bowl XLI](#) in Miami., provides attackers with built-in Web traffic and minimizes the need for lures through email, instant messaging or Web posts.

6. Rise in targeted Web 2.0 special interest attacks—hackers targeting specific groups of people based on interests and profile

Web 2.0 has spawned a proliferation of Web users that visit chat rooms, social networking sites, and special interest Web sites such as travel sites, automotive, and more. These sites provide hackers with potential victims that fall within a certain age group, wealth bracket, or people with particular purchasing habits. In 2008, Websense researchers predict targeted attacks will rise toward specific social networking or special interest sites that have a higher probability of delivering a payoff.

7. Morphing JavaScript to evade anti-virus scanners

Hackers are upping the ante with evasion techniques that use poly-morphic JavaScript (Polyscript) – which means that a uniquely-coded Web page is served up for each visit by a user to a malicious Web site. By changing the code every visit, signature-based security scanning technologies have difficulty detecting Web pages as malicious and hackers can extend the length of time their malicious site evades detection.

8. Data concealment methods increase in sophistication

Websense predicts an increased use of crypto-virology and sophistication in data concealment including the use of steganography, embedding data within standard protocols, and potentially within media files. Toolkits widely available on the Web will be used to embed proprietary information and steal data.

9. Global law enforcement will crack down on key hacker groups and individuals

In 2007, large-scale Internet-based attacks garnered the attention of law enforcement officials around the world. Websense anticipates that through the global cooperation of enforcement agencies, in 2008 the biggest crackdown and arrests of key members of a hacker group will occur.

10. Vishing and voice spam will combine and increase

The vast cell phone user population has grown into a lucrative market to exploit with spamming and “vishing” for financial gain. To date, researchers have seen an increased number of vishing attacks but not a lot spam—or pro-active automated calling. In 2008 Websense predicts that “vishing” or the practice of using social engineering and Voice over IP (VoIP) to gain personal and financial information and voice spam will combine and increase—users will receive automated voice calls on LAN lines with voice spam to lure them to input their credentials through the telephone.

About Websense Security Labs

Overview

Websense Security Labs is the security research arm of Websense that discovers, investigates and reports on advanced Internet threats. Unlike other research labs, Websense has an unparalleled knowledge of malware and where it resides on the Web. This allows Websense to detect and block new threats that traditional security research methods miss, enabling an organization to protect their sensitive content from theft, compromise, or inappropriate use.

Recognized as a world leader in security research, Websense Security Labs publishes findings to hundreds of security partners, vendors, media outlets, military and other organizations around the world 24 hours a day, seven days a week. With a team of Global Threat Experts and operations in the Americas, Europe, Middle East, Africa and Asia Pacific, Websense Security Labs provides continuous monitoring of all Internet threats including Internet-borne threats, stemming from Web, email, Instant Messaging and Peer-to-Peer file-sharing.

The Websense Security Labs team has expanded to include an advanced content research team, and a dedicated research team that covers email threats. By combining Web and email research, Websense has a unique, early insight into email and web threats that provides comprehensive protection for all customers across both protocols.

Websense Security Labs – a Pioneer in Emerging Threat Protection

- First to market with phishing protection
- First to market with drive-by and backchannel spyware protection
- First to market with bot network protection
- First to market with crimeware/keylogger protection

Websense Security Labs researchers gather threat intelligence with Websense ThreatSeeker™ technology which scans more than 600 million Web sites per week searching for malicious code, along with Websense's On Demand Services, which scans more than 350 million emails per week for email security threats. The Websense Security Labs research team, credited with finding several high-impact Web exploits and zero-days, sends out an average of 70 security updates per day, to protect more than 42 million employees from external and internal computer security threats.

Security Alerts

Register with Websense Security Labs to receive FREE security warnings about malicious internet events, including spyware, phishing, pharming, and corrupted Web sites. To subscribe to the latest threat research and alerts, please visit: www.websensesecuritylabs.com

Blog Highlights

For more information, check out our blog: <http://www.WebsenseSecurityLabs.com/blog>

© 2007 Websense, Inc. All rights reserved. Websense, Websense Enterprise, and other Websense trademarks are registered trademarks or trademarks of Websense, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners.